

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日

Date of Application:

2000年 6月30日

出 願 番 号

Application Number:

特願2000-199265

願 人

Applicant (s):

富士通株式会社

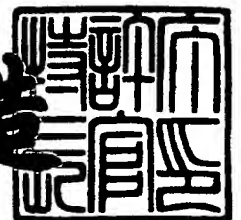


CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月20日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3087522

【書類名】 特許願

【整理番号】 0051230

【提出日】 平成12年 6月30日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G06F 12/14
G06F 9/24 320

【発明の名称】 プログラムインストール方法、プログラムインストールシステム、プログラム実行装置及び記憶媒体

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 塩原 知美

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 川崎 雄介

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 橋本 繁

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094514

【弁理士】

【氏名又は名称】 林 恒▲徳▼

【代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 プログラムインストール方法、プログラムインストールシステム、プログラム実行装置及び記憶媒体

【特許請求の範囲】

【請求項 1】 プログラムの署名データを受信するステップと、
前記署名データからインストールされている他のプログラムとの干渉をチェックするステップと、

干渉の無いプログラムのインストールを許可するステップとを有することを
特徴とするプログラムインストール方法。

【請求項 2】 前記チェックステップは、
前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックするステップであることを
特徴とする請求項 1 のプログラムインストール方法。

【請求項 3】 前記許可されたプログラムの前記署名データを登録するステップを更に有することを
特徴とする請求項 1 のプログラムインストール方法。

【請求項 4】 前記受信ステップは、
前記署名データと前記プログラムとを受信するステップであることを
特徴とする請求項 1 のプログラムインストール方法。

【請求項 5】 前記受信ステップは、
前記署名データを受信するステップであり、
前記インストールを許可するステップは、
前記許可されたプログラムを要求し、前記プログラムを受信するステップであることを
特徴とする請求項 1 のプログラムインストール方法。

【請求項 6】 インストールされたプログラムを格納するメモリと、
前記プログラムを実行するプロセッサとを有し、
前記プロセッサは、プログラムの署名データを受信し、前記署名データからインストールされている他のプログラムとの干渉をチェックし、干渉の無いプログ

ラムのインストールを許可することを
特徴とするプログラム実行装置。

【請求項 7】前記プロセッサは、
前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックすることを
特徴とする請求項 6 のプログラム実行装置。

【請求項 8】前記プロセッサは、
前記許可されたプログラムの前記署名データを登録することを
特徴とする請求項 6 のプログラム実行装置。

【請求項 9】プログラム要求に応じて少なくともプログラムの署名データをアップロードする第 1 の装置と、
前記署名データを受信し、前記署名データからインストールされている他のプログラムとの干渉をチェックし、干渉の無いプログラムのインストールを許可する第 2 の装置とを有することを
特徴とするプログラムインストールシステム。

【請求項 10】プログラムの署名データを受信するプログラムと、
前記署名データからインストールされている他のプログラムとの干渉をチェックするプログラムと、
干渉の無いプログラムのインストールを許可するプログラムとを記憶した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、プログラムをインストールするプログラムインストール方法、プログラムインストールシステム、プログラム実行装置及びその記憶媒体に関し、特に、既存のプログラムとの干渉を防止する機能を持つプログラムインストール方法、プログラムインストールシステム、プログラム実行装置及びその記憶媒体に関する。

【0002】

【従来の技術】

電子商取引等あらゆる分野で、よりセキュリティーの高い装置が求められている。特に、プログラムを実行するプログラム実行装置では、プログラムをインストールでき、インストールされたプログラムを実行するため、複数のアプリケーションプログラムを自由にインストールできる。

【0003】

OS等がメモリ管理を行う装置では、ワークメモリ領域の資源管理を行う機能を有するが、新たにインストールされたプログラムが他のプログラムと干渉しても、チェックする機能を有していなかった。

【0004】

【発明が解決しようとする課題】

従来の技術では、インストールされたプログラムが、他のプログラムの解析等を行っても、これをチェックすることができないという問題があり、セキュリティーの高いプログラムをインストールした装置には、新たなプログラムをインストールすることは禁止せざる得ない。

【0005】

例えば、電子商取引の電子マネー処理プログラムを搭載した装置では、データとして、暗号鍵等のセキュリティーデータを有しているため、不正なプログラムがインストールされると、この不正なプログラムにより、セキュリティーデータの書き換えや読み出しが行われてしまう。このため、セキュリティーの高いプログラムをインストールした後は、他のプログラムのインストールを禁止していた。

【0006】

しかし、種々のプログラムを1台の装置で実行することが望まれているため、インストールが禁止された場合、新たなプログラムは、他の装置を使用するという無駄が生じるという問題がある。例えば、電子商取引の分野では、電子マネー、デビットカード、クレジットカードを決済処理する複数のアプリケーションを1台の装置で取り扱いたいという要求に答えることが出来ない。

【0007】

従って、本発明の目的は、新規にインストールしても、プログラム間の干渉を

防止するためのプログラムインストール方法、プログラムインストールシステム、プログラム実行装置及び記憶媒体を提供するにある。

【0008】

本発明の他の目的は、新規にインストールしても、プログラムのセキュリティを維持するためのプログラムインストール方法、プログラムインストールシステム、プログラム実行装置及び記憶媒体を提供するにある。

【0009】

更に、本発明の他の目的は、不正なプログラムのインストールを防止するためのプログラムインストール方法、プログラムインストールシステム、プログラム実行装置及び記憶媒体を提供することにある。

【0010】

【課題を解決するための手段】

この目的の達成のため、本発明のプログラムインストール方法は、プログラムの署名データを受信するステップと、前記署名データからインストールされている他のプログラムとの干渉をチェックするステップと、干渉の無いプログラムのインストールを許可するステップとを有する。

【0011】

本発明では、インストールするプログラムから署名データを申告させ、これにより、プログラム間の干渉チェックを行い、認証を行って、干渉のあるプログラムのインストールを阻止する。又、干渉の無いプログラムのインストールを実行する。このため、セキュリティの高いプログラムを保護しつつ、新規なプログラムのインストールが可能となる。

【0012】

又、本発明では、前記チェックステップは、前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックするステップであることにより、容易にプログラム間の干渉をチェックできる。

【0013】

更に、本発明では、前記許可されたプログラムの前記署名データを登録するス

テップを更に有することにより、署名データによる干渉チェックが可能となる。

【0014】

更に、本発明では、前記受信ステップは、前記署名データと前記プログラムとを受信するステップであることにより、インストールが効率的に可能となり、小さなサイズのプログラムのインストールに有効である。

【0015】

更に、本発明では、受信ステップは、前記署名データを受信するステップであり、前記インストールを許可するステップは、前記許可されたプログラムを要求し、前記プログラムを受信するステップであることにより、許可されないプログラムの無用な転送を防止でき、大きなサイズのプログラムのインストールに有効である。

【0016】

【発明の実施の形態】

以下、本発明を、プログラム実行装置、インストール方法、他の実施の形態に分けて、説明する。

〔プログラム実行装置〕

図1は、本発明の一実施の形態のプログラム実行装置を使用したシステムの構成図であり、図2は、プログラム実行装置の説明図であり、図3は、このプログラム実行装置の構成図である。

【0017】

図1は、プログラム実行装置を使用したシステム構成図であり、POSシステムを示している。LAN等のネットワーク35に、管理用パーソナルコンピュータ15と、ストアコントローラ20と、複数のPOS10が接続されている。各POS10には、ICカードリーダー/ライター30が接続されている。ストアコントローラ20と、複数のPOS10とには、プログラム実行装置としての決済用LSI（IFDという）ボード2が設けられ、決済データを直接やりとりする。

【0018】

図2に示すものでは、システムLSIボード2は、カード決済用LSIであり、デビットカード決済機能40、クレジットカード決済機能41、電子マネー決

済機能42、その他のサービス機能43を有する。このため、LSIボード2には、ICカードリーダー/ライター30と、磁気カードリーダー31と、表示及びキー32とが接続される。又、必要に応じて、レシートプリンタ33が接続される。これらの決済機能40～43は、LSI2のCPU65（図3にて後述する）のプログラムの実行により、実現され、このため、各決済プログラムがインストールされる。

【0019】

従って、このLSI2を搭載することにより、各種の電子装置50～57に、カード決済機能を付与できる。これらの電子装置は、例えば、POS用リーダー/ライター50、統合端末51、モバイル端末52、ATM（自動テラマシ）53、自動販売機54、PDA（パーソナル機器）55、携帯電話56、PC（パーソナルコンピュータ）57である。

【0020】

このカード決済のためのシステムLSIボード2を、図3により説明する。システムLSIボード2には、システムLSI1が搭載される。システムLSI1は、スマートカードコントローラ60と、MS制御回路61と、LCD制御回路62と、マトリクスKB制御回路63と、メモリコントローラ64と、CPU65と、シリアル入出力ポート66～69と、バス80とを有する。

【0021】

スマートカードコントローラ60は、ICカードリーダー/ライター30を介しICカード（スマートカードという）のデータのリード/ライトを行う。MS制御回路61は、MS（磁気ストライプ）リーダー31の制御を行う。LCD制御回路62は、LCD（液晶ディスプレイ）32-1の表示制御を行う。マトリクスKB制御回路63は、テンキー32-2の入力を認識する。メモリコントローラ64は、ボード1上の各種メモリ（ROM70、SRAM71、FLASH72、SDRAM73）との入出力制御を行う。シリアルポート66～69は、シリアルデータの入出力を行うため、ボード1のドライバ74～76に接続される。これらは、いずれもCPUバス80に接続される。

【0022】

各決済用アプリケーションプログラムは、図1の管理用パーソナルコンピュータ15からFLASH72にインストールされ、CPU65が指定された決済に応じて、対応する決済用アプリケーションプログラムを実行する。決済用データには、パスワード、金額、口座番号等のセキュリティの必要なデータを含むため、暗号化され、決済用アプリケーションプログラムには、決済データの暗号化のための暗号鍵等を有する。

【0023】

図1に戻り、システムの動作を説明する。顧客のICカード34-1は、IFD2を介しPOS用ICカード34-2と交信し、POS用ICカード34-2は、IFD2、ターミナルコントローラ11、ネットワーク35、ターミナルコントローラ11、IFD2を介しストアコントローラ20のICカード34-2と交信する。

【0024】

例えば、ICカードで電子決済を行う場合には、顧客のICカード34-1のデータは、IFD2を介しPOS用ICカード34-2に格納される。その後、POS用ICカード34-2の格納データは、IFD2、ターミナルコントローラ11、ネットワーク35、ターミナルコントローラ11、IFD2を介しストアコントローラ20のICカード34-2に格納される。

【0025】

このシステムでは、IFD2により、電子決済データのルートがクローズしているため、決済データ（パスワード、口座番号、残高等）が漏れるおそれがないため、安全性が高い。

【0026】

しかし、前述のように、電子商取引の電子マネー処理プログラムを搭載した装置では、データとして、暗号鍵等のセキュリティデータを有しているため、不正なプログラムがインストールされると、この不正なプログラムにより、セキュリティデータの書き換えや読み出しが行われてしまう。一方、インストールを禁止すると、新たに取り扱う電子決済のためのアプリケーションプログラムをインストールできないため、不便である。従って、後述する本発明のインストール方法

は、このような用途に特に有効である。勿論、他の用途のプログラム実行装置にも適用できる。

【インストール方法】

図4は、本発明の一実施の形態のインストール方法の説明図、図5は、図4のアプリケーションマネージャ3に登録されたアプリケーションプログラムの管理情報の説明図、図6は、ダウンロードプログラム6の署名情報7の説明図、図7は、図4のプログラマネージャの処理フロー図、図8は、図4のアプリケーションマネージャ3のチェック処理フロー図である。

【0027】

図4に示すように、LSI1は、プログラマネージャ4と、アプリケーションマネージャ3とが設けられている。いずれも、プログラムの実行により実現される。プログラマネージャ4は、プログラム全体の管理を行うものであり、インストールの制御も行う。アプリケーションマネージャ3は、アプリケーションプログラムが管理情報に従い動作しているかをチェックするものであり、本発明では、インストール時にプログラムの干渉をチェックし、認証を行う。

【0028】

パーソナルコンピュータ15は、通信制御部5と、ダウンロードプログラム6とを有する。ダウンロードプログラム6には、本発明では、署名データ7が設けられている。署名データ7は、図6に示すように、そのプログラムがアクセスするメモリ情報と、走行レベルと、プログラムID等からなる。メモリ情報は、属性（リード／ライト／コード）の領域先頭アドレスと、領域レンジからなる。リードは、読み出しであり、ライトは書き込みであり、コードは、プログラムの格納される場所を示す。

【0029】

一方、アプリケーションマネージャ3には、図5に示す管理情報が登録されている。アプリケーションNo. 100には、インストールされたアプリケーションプログラムのIDが登録されている。アクセス許可テーブル110には、各インストールされたアプリケーションプログラム毎に、アプリケーションの走行レベルと、参照走行レベルが格納される。走行レベルは、走行レベルのテーブル1

20のポインタであり、テーブル120には、前述のメモリ情報を登録してある。参照走行レベルは、そのアプリケーションが参照するライブラリ（例えば、関数計算）の走行レベルである。

【0030】

図4に戻り、インストール動作を説明する。

【0031】

①プログラマネージャ4から通信制御部5にプログラム要求を発する。

【0032】

②通信制御部5は、指定されたダウンロードプログラム6を選択する。このダウンロードプログラム6には、署名データ7が含まれる。

【0033】

③ダウンロードプログラム6を暗号化し、プログラマネージャ4にアップロードする。

【0034】

④プログラマネージャ4は、図7に示すように、ダウンロードプログラム6を復号し、チェックし、署名データを取り出す。

【0035】

⑤プログラマネージャ4は、取り出した署名データ7をアプリケーションマネージャ3に通知する。

【0036】

⑥アプリケーションマネージャ3は、図8で詳述するように、図5の管理情報を参照して、署名データにより、プログラム間の干渉をチェックする。

【0037】

⑦アプリケーションマネージャ3は、チェック結果（認証結果）をプログラマネージャ4に通知する。

【0038】

⑧プログラマネージャ4は、インストール許可かを判定し、許可なら、ワークエリアに展開されたダウンロードプログラム6を、メモリの指定領域にセットする。

【0039】

⑨プログラムをセットすると、プログラムマネージャ4は、アプリケーションマネージャ3に完了を通知する。アプリケーションマネージャ4は、前述の署名データ7を管理情報に登録する。

【0040】

一方、不許可の場合には、プログラムマネージャ4は、ワークエリアに展開されたダウンロードプログラム6を、消去する。即ち、インストールは実行されない。

【0041】

このようにして、インストールするプログラムからメモリ情報を含む署名データを申告させ、これにより、プログラム間の干渉チェックを行い、認証を行って、干渉のあるプログラムのインストールを阻止する。又、干渉の無いプログラムのインストールを実行する。このため、セキュリティの高いプログラムを保護しつつ、新規なプログラムのインストールが可能となる。

【0042】

又、前述の認証に使用される署名データは、メモリ情報であり、そのままアプリケーションマネージャ4の管理情報に利用できる。このため、署名データを申告させても、申告内容を有効に利用できる。

【0043】

次に、プログラムマネージャ4の前述のインストール処理④～⑨を、図7により説明する。

【0044】

(S10) 暗号化されたダウンロードプログラム6を復号化し、復号が正常に行われたかを判定する。復号が正常に行われていない場合には、認証NGをパーソナルコンピュータ15に通知し、異常終了する。例えば、ワーク領域に展開されたダウンロードプログラムを消去する。

【0045】

(S11) 復号が正常なら、ダウンロードプログラム6の署名データ7を取り出し、アプリケーションマネージャ3に認証を依頼する。アプリケーションマネ

ージャ 3 は、後述する図 8 の処理により、認証結果を通知する。

【 0 0 4 6 】

(S 1 2) 通知された認証結果が O K でない場合には、認証 N G をパーソナルコンピュータ 1 5 に通知し、異常終了する。例えば、ワーク領域に展開されたダウンロードプログラムを消去する。

【 0 0 4 7 】

(S 1 3) 認証結果が O K なら、プログラムを指定領域にロードする。ロードが正常に終了しない場合には、認証 N G をパーソナルコンピュータ 1 5 に通知し、異常終了する。

【 0 0 4 8 】

(S 1 4) ロードが正常に終了すると、アプリケーションマネージャ 3 に署名データ 7 をセットし、プログラム情報をセットし、認証 O K をパーソナルコンピュータ 1 5 に通知し、インストールを終了する。

【 0 0 4 9 】

次に、図 8 により、ステップ S 1 1 のアプリケーションマネージャ 3 の認証処理を説明する。

【 0 0 5 0 】

(S 2 0) 署名データのプログラム I D と図 5 の登録されたプログラム I D とを比較し、アプリケーション N o . が新規かを判定する。新規でない場合には、既存プログラムが上書きされてしまうため、認証 N G を通知する。即ち、不正な上書きを防止する。

【 0 0 5 1 】

(S 2 1) 署名データの参照走行レベルは、既存かを判定する。参照走行レベルは、参照するライブラリを指定するため、参照走行レベルが既存でない場合は、参照ライブラリが存在しないため、認証 N G を通知する。即ち、参照不可の異常終了するプログラムを排除する。

【 0 0 5 2 】

(S 2 2) 次に、アプリケーション走行レベルが新規かを判定する。走行レベルが新規でないでは、既存プログラムと干渉するため、認証 N G を通知する。

【 0 0 5 3 】

(S 2 3) アプリケーション走行レベルが新規でない場合には、メモリ情報に示すアドレスから、装置に存在しないアドレスをアクセスするかを判定し、存在しないアドレスなら、認証 N G を通知する。即ち、アクセスできないプログラムを排除する。

【 0 0 5 4 】

(S 2 4) メモリ情報から各種レジスタ (I / O) 領域をコード領域 (プログラム格納領域) とするものかを判定する。レジスタは、各プログラムで使用するため、書き換えられる。このため、このようなプログラムをロードしても、このプログラムのセキュリティを維持できないため、認証 N G を通知する。

【 0 0 5 5 】

(S 2 5) メモリ情報のリード、リード / ライト領域が、既にインストールされているアプリケーションのコード領域をデータ領域として、リード / ライトするかを判定する。メモリ情報のリード、リード / ライト領域が、既にインストールされているアプリケーションのコード領域をデータ領域として、リード / ライトする場合は、このプログラムにより、既にインストールされているアプリケーションプログラム自体のリード / ライトが行われ、干渉が生じる。これにより、既存のアプリケーションのセキュリティを維持できないため、認証 N G を通知する。

【 0 0 5 6 】

(S 2 6) コード領域として指定されているサイズと、実際に受信したプログラムサイズが一致するかを判定する。一致しない場合には、認証 N G を通知する。一方、一致する場合には、アプリケーションマネージャ 3 の管理情報にそのレベルを追加し、認証 O K を通知する。

【 0 0 5 7 】

(S 2 7) この認証結果を、プログラムマネージャに通知し、終了する。

【 0 0 5 8 】

このようにして、プログラム間の干渉をメモリ情報からチェックし、干渉がある場合には、セキュリティが維持できないため、インストールを実行しない。一

方、干渉のないプログラムはインストールを許可する。このため、セキュリティの高いプログラムを保護しつつ、新規なプログラムのインストールが可能となる。

【0059】

又、インストールされるプログラムのセキュリティが維持できるかもチェックしている。このため、インストールされたプログラムのセキュリティも維持できる。

【0060】

〔他の実施の形態〕

図9は、本発明の他の実施の形態のインストール処理の説明図である。図4の実施の形態では、一度に、署名を含むプログラム全体をダウンロードするのに対し、この実施の形態は、署名データだけを先ず要求し(①)、署名データをアップロードし、認証し(③～⑧)、許可対象である場合には、プログラムを要求し、引き続きプログラム自体のアップロード、書き込みを行う。このメリットは、時間をかけてNGのプログラムをダウンロードする手間を防止でき、プログラムサイズが大きい場合に有効である。逆に、プログラムサイズが小さい場合には、図4のように、署名とプログラムを一度にダウンロードする方法が効率的である。

【0061】

上述の実施の態様の他に、本発明は、次のような変形が可能である。

(1) セキュリティの高いプログラムとして、電子マネー決済プログラムで説明したが、デビットカード決済プログラム、クレジットカード決済プログラム等の他の前述のセキュリティの必要なプログラムにも適用できる。

(2) プログラム実行装置を、決済用システムLSIで説明したが、他のプログラム実行装置に適用できる。

【0062】

以上、本発明を実施の形態により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【0063】

〔付記〕

（付記 1）プログラムの署名データを受信するステップと、前記署名データからインストールされている他のプログラムとの干渉をチェックするステップと、干渉の無いプログラムのインストールを許可するステップとを有することを特徴とするプログラムインストール方法。

【 0 0 6 4 】

（付記 2）前記チェックステップは、前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックするステップであることを特徴とする付記 1 のプログラムインストール方法。

【 0 0 6 5 】

（付記 3）前記許可されたプログラムの前記署名データを登録するステップを更に有することを特徴とする付記 1 のプログラムインストール方法。

【 0 0 6 6 】

（付記 4）前記受信ステップは、前記署名データと前記プログラムとを受信するステップであることを特徴とする付記 1 のプログラムインストール方法。

【 0 0 6 7 】

（付記 5）前記受信ステップは、前記署名データを受信するステップであり、前記インストールを許可するステップは、前記許可されたプログラムを要求し、前記プログラムを受信するステップであることを特徴とする付記 1 のプログラムインストール方法。

【 0 0 6 8 】

（付記 6）インストールされたプログラムを格納するメモリと、前記プログラムを実行するプロセッサとを有し、前記プロセッサは、プログラムの署名データを受信し、前記署名データからインストールされている他のプログラムとの干渉をチェックし、干渉の無いプログラムのインストールを許可することを特徴とするプログラム実行装置。

【 0 0 6 9 】

（付記 7）前記プロセッサは、前記署名データのメモリ使用情報と、前記イン

ストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックすることを特徴とする付記 6 のプログラム実行装置。

【0070】

(付記 8) 前記プロセッサは、前記許可されたプログラムの前記署名データを登録することを特徴とする付記 6 のプログラム実行装置。

【0071】

(付記 9) 前記プロセッサは、前記署名データと前記プログラムとを受信することを特徴とする付記 6 のプログラム実行装置。

【0072】

(付記 10) 前記プロセッサは、前記署名データを受信し、前記インストールを許可した時に、前記許可されたプログラムを要求し、前記プログラムを受信することを特徴とする付記 6 のプログラム実行装置。

【0073】

(付記 11) プログラム要求に対し、少なくともプログラムの署名データをアップロードするステップと、前記プログラムの署名データを受信するステップと、前記署名データからインストールされている他のプログラムとの干渉をチェックするステップと、干渉の無いプログラムのインストールを許可するステップとを有することを特徴とするプログラムインストール方法。

【0074】

(付記 12) 前記チェックステップは、前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックするステップであることを特徴とする付記 11 のプログラムインストール方法。

【0075】

(付記 13) 前記許可されたプログラムの前記署名データを登録するステップを更に有することを特徴とする付記 11 のプログラムインストール方法。

【0076】

(付記 14) 前記受信ステップは、前記署名データと前記プログラムとを受信するステップであることを特徴とする付記 11 のプログラムインストール方法。

【0077】

(付記15) 前記受信ステップは、前記署名データを受信するステップであり、前記インストールを許可するステップは、前記許可されたプログラムを要求し、前記プログラムを受信するステップであることを特徴とする付記11のプログラムインストール方法。

【0078】

(付記16) プログラム要求に対し、少なくともプログラムの署名データをアップロードする第1の装置と、前記プログラムの署名データを受信し、前記署名データからインストールされている他のプログラムとの干渉をチェックし、干渉の無いプログラムのインストールを許可する第2の装置とを有することを特徴とするプログラムインストールシステム。

【0079】

(付記17) 前記第2の装置は、前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックすることを特徴とする付記16のプログラムインストールシステム。

【0080】

(付記18) 前記第2の装置は、前記許可されたプログラムの前記署名データを登録することを特徴とする付記16のプログラムインストールシステム。

【0081】

(付記19) 前記第2の装置は、前記署名データと前記プログラムとを受信することを特徴とする付記16のプログラムインストールシステム。

【0082】

(付記20) 前記第2の装置は、前記署名データを受信し、前記インストールを許可した時に、前記許可されたプログラムを要求し、前記プログラムを受信することを特徴とする付記16のプログラムインストールシステム。

【0083】

(付記21) プログラムの署名データを受信するプログラムと、前記署名データからインストールされている他のプログラムとの干渉をチェックするプログラムと、干渉の無いプログラムのインストールを許可するプログラムとを記憶した

記憶媒体。

【0084】

(付記22) 前記チェックプログラムは、前記署名データのメモリ使用情報と、前記インストールされている他のプログラムのメモリ使用情報から、前記干渉をチェックするプログラムであることを特徴とする付記21の記憶媒体。

【0085】

(付記23) 前記許可されたプログラムの前記署名データを登録するプログラムを更に有することを特徴とする付記21の記憶媒体。

【0086】

(付記24) 前記受信プログラムは、前記署名データと前記プログラムとを受信するプログラムであることを特徴とする付記21の記憶媒体。

【0087】

(付記25) 前記受信プログラムは、前記署名データを受信するプログラムであり、前記インストールを許可するプログラムは、前記許可されたプログラムを要求し、前記プログラムを受信するプログラムであることを特徴とする付記21の記憶媒体。

【0088】

【発明の効果】

以上説明したように、本発明によれば、インストールするプログラムから署名データを申告させ、これにより、プログラム間の干渉チェックを行い、認証を行って、干渉のあるプログラムのインストールを阻止する。又、干渉の無いプログラムのインストールを実行する。このため、セキュリティの高いプログラムを保護しつつ、新規なプログラムのインストールが可能となる。

【図面の簡単な説明】

【図1】

本発明の一実施の形態のプログラム実行装置を使用したシステムのブロック図である。

【図2】

図1のプログラム実行装置の説明図である。

【図 3】

図 1 のプログラム実行装置のブロック図である。

【図 4】

本発明の一実施の形態のインストール処理の説明図である。

【図 5】

図 4 のアプリケーションマネージャの管理情報の説明図である。

【図 6】

図 4 の署名データの説明図である。

【図 7】

図 4 のプログラムマネージャのインストール処理フロー図である。

【図 8】

図 7 のアプリケーションマネージャの認証処理フロー図である。

【図 9】

本発明の他の実施の形態のインストール処理フロー図である。

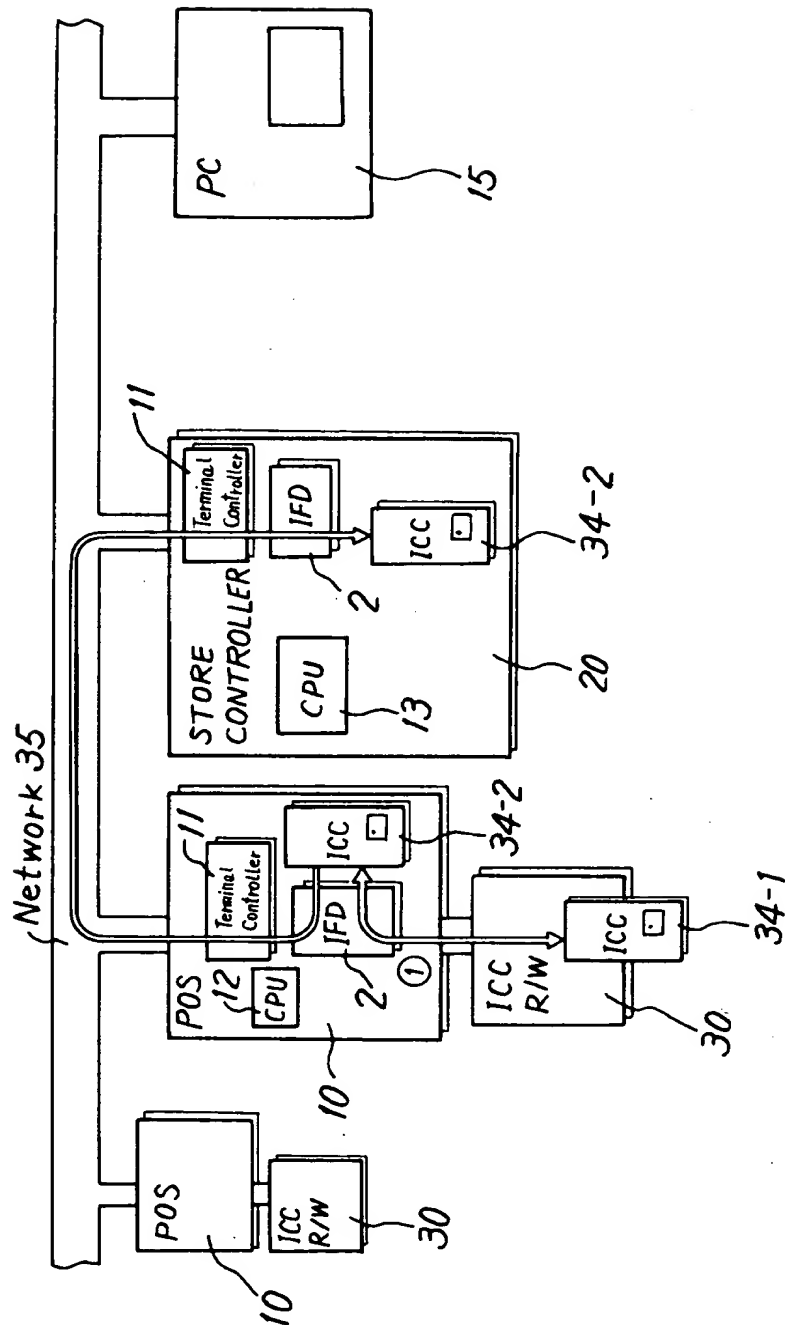
【符号の説明】

- 1 システム L S I
- 2 L S I ボード
- 3 アプリケーションマネージャ
- 4 プログラムマネージャ
- 5 通信制御部
- 6 ダウンロードプログラム
- 7 署名データ

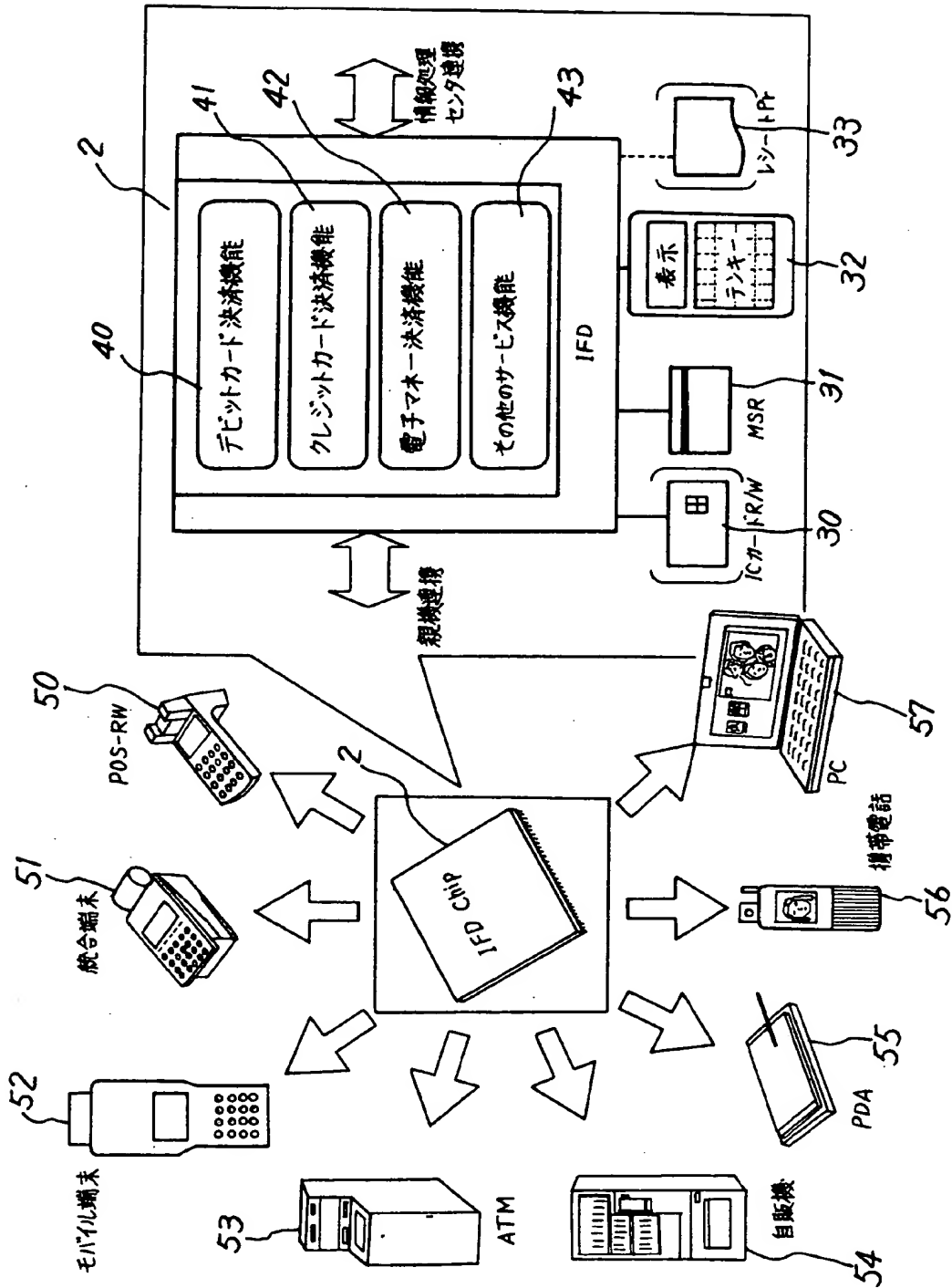
【書類名】

図面

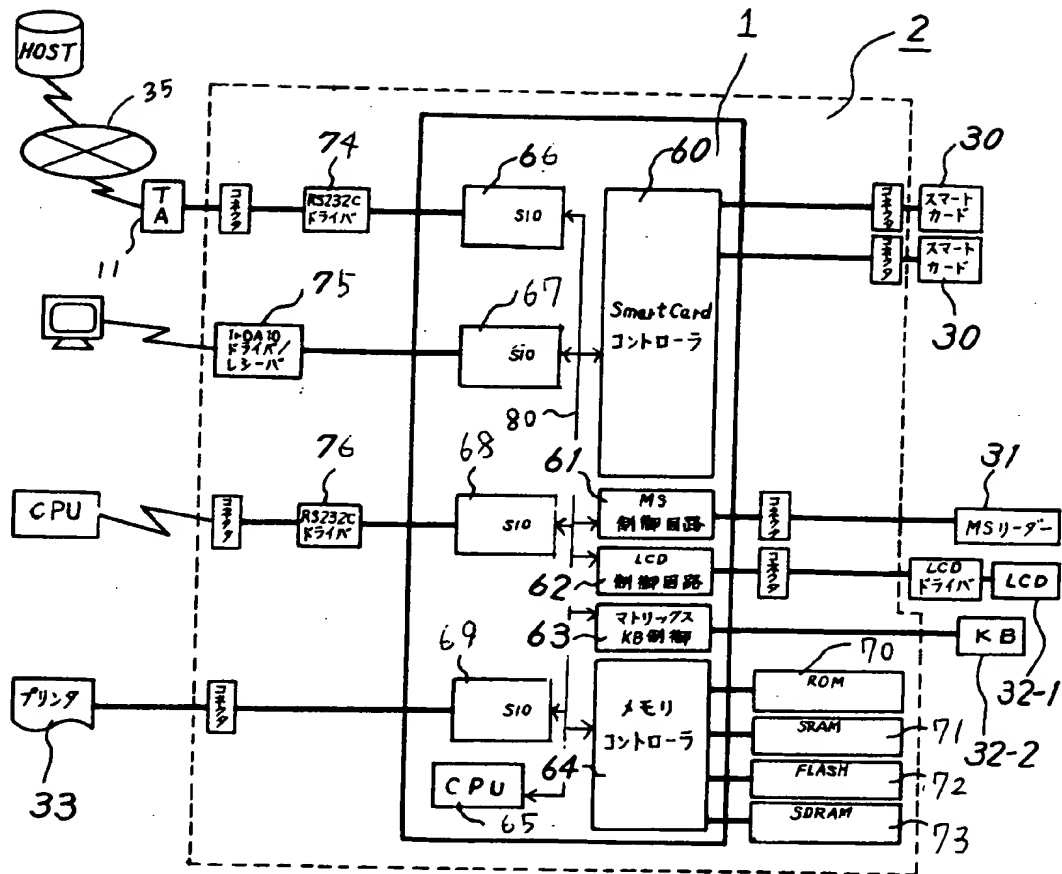
【図 1】



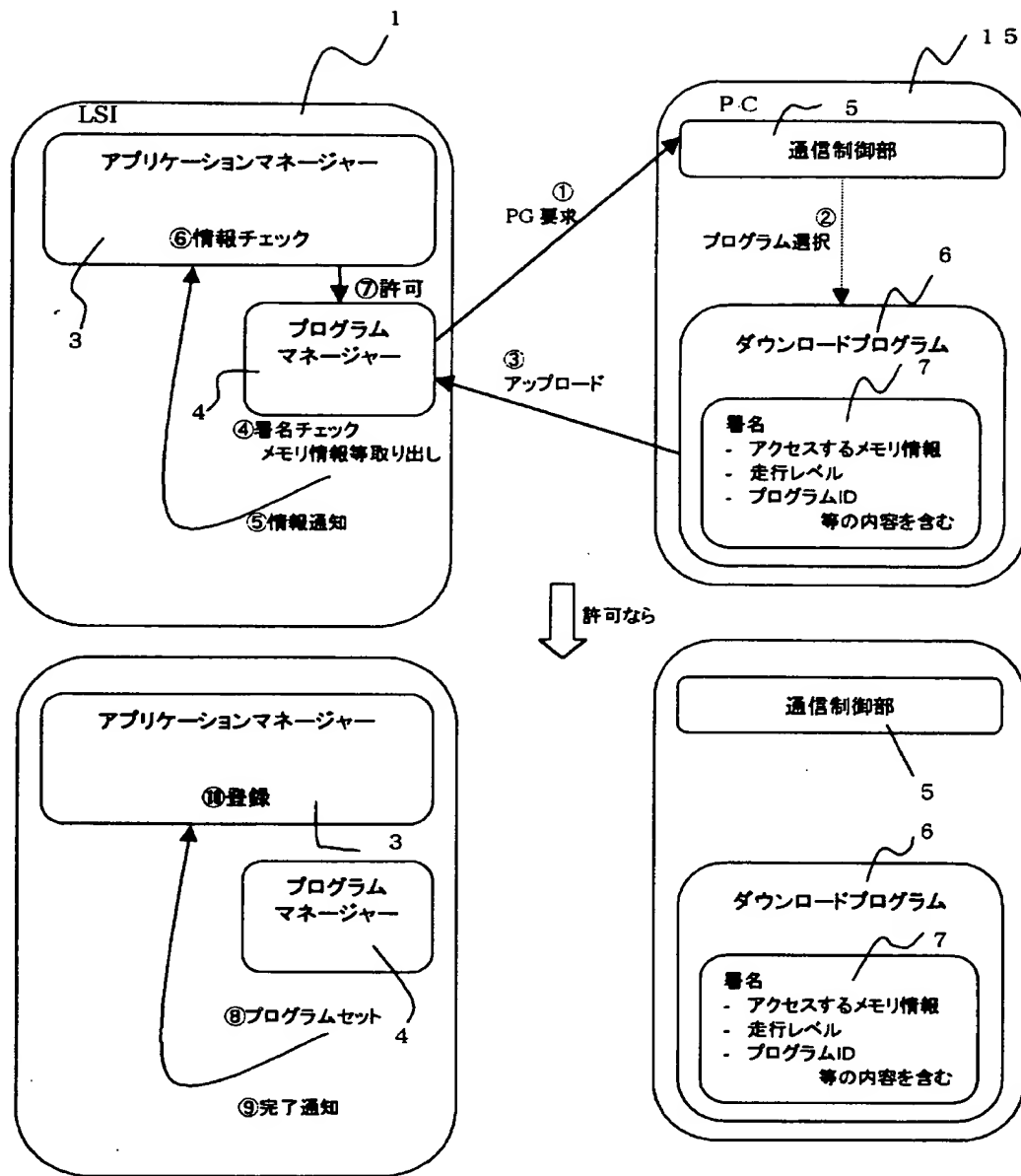
【図2】



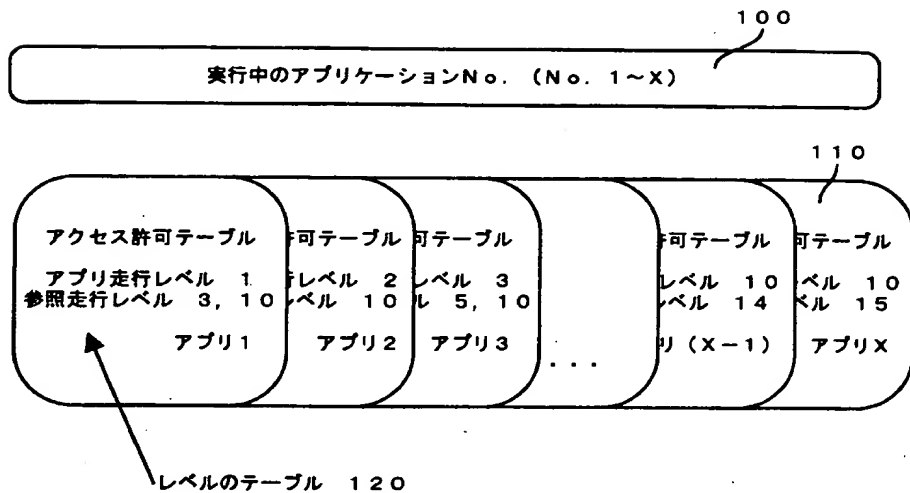
【図3】



【図 4】



【図 5】



走行レベル1		
属性(リード/ライト/コード)	領域先頭アドレス	領域レンジ
リード	xxxx xxxxxH	0000 0100 H
リード/ライト	xxxx xxxxxH	0001 0000 H
リード/ライト	xxxx xxxxxH	0001 0000 H
リード/ライト	xxxx xxxxxH	0000 8000 H
コード	xxxx xxxxxH	0010 0000 H
コード	xxxx xxxxxH	0000 1000 H

走行レベル2		
属性(リード/ライト/コード)	領域先頭アドレス	領域レンジ
リード/ライト	xxxx xxxxxH	0001 0000 H
リード/ライト	xxxx xxxxxH	0000 8000 H
コード	xxxx xxxxxH	0010 0000 H

...

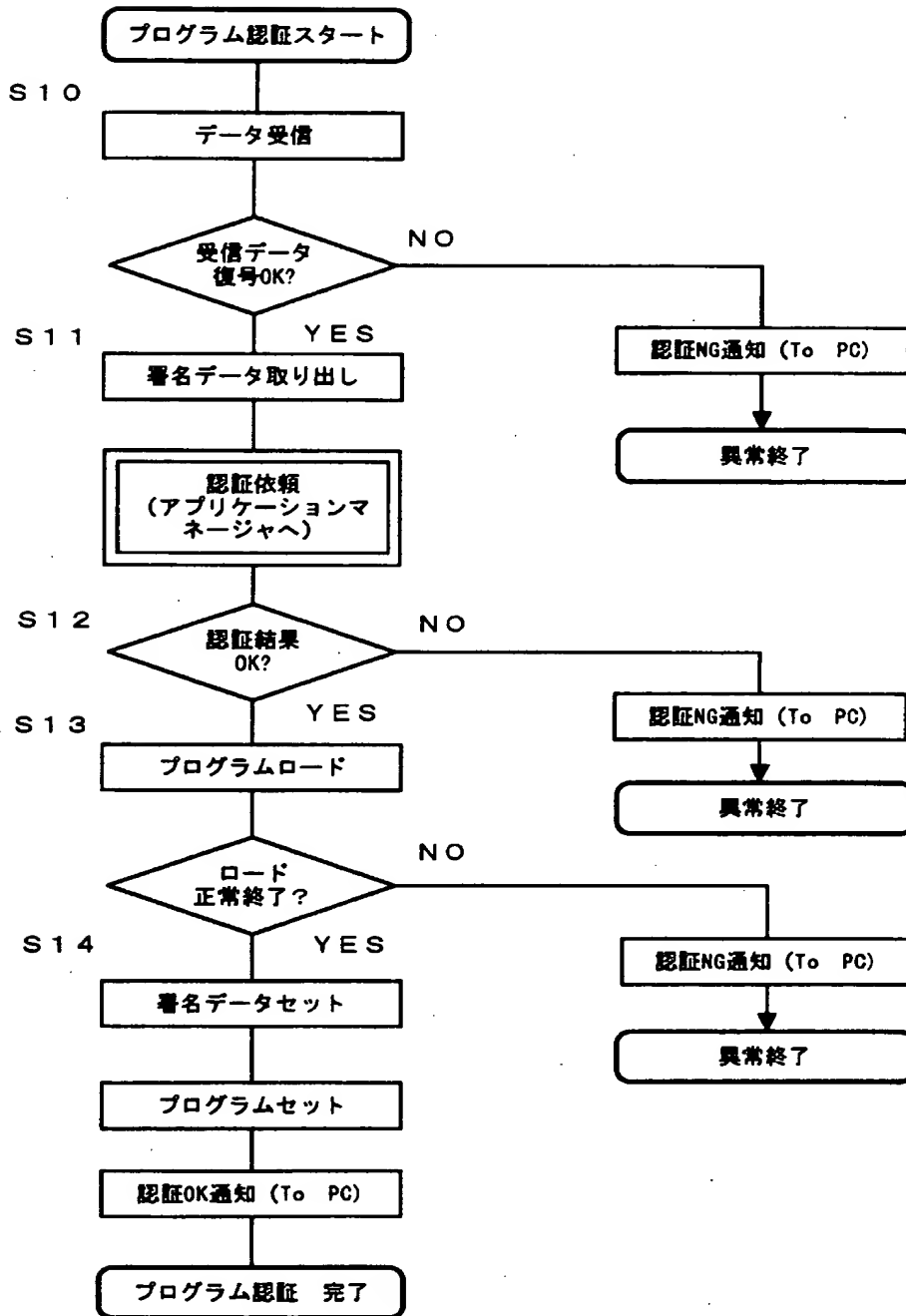
走行レベル15		
属性(リード/ライト/コード)	領域先頭アドレス	領域レンジ
リード	xxxx xxxxxH	0000 0100 H
リード	xxxx xxxxxH	0000 0080 H
リード/ライト	xxxx xxxxxH	0000 0080 H
コード	xxxx xxxxxH	0010 0000 H

【図 6】

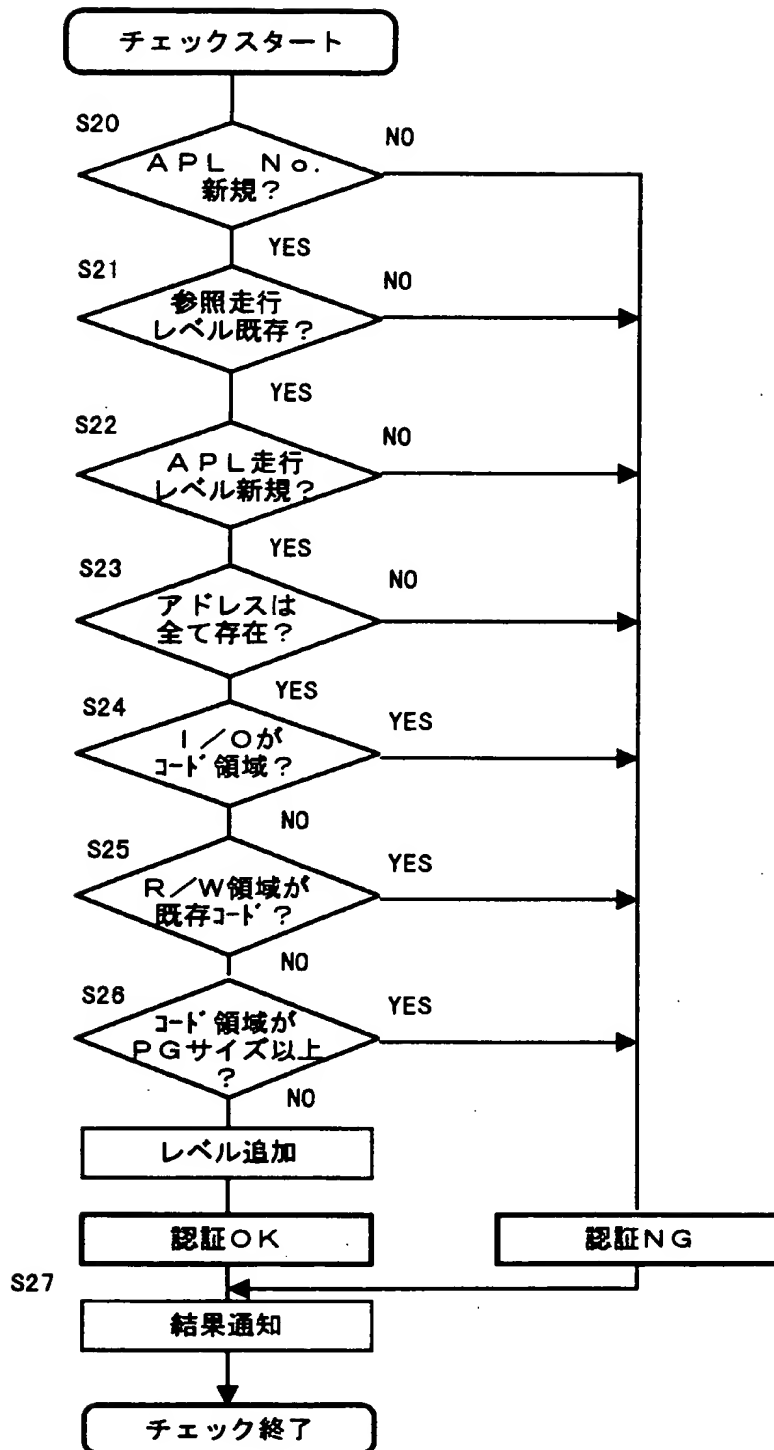
プログラム ID		
走行レベル A		
属性(リード/ライト/コード)	領域先頭アドレス	領域レンジ
リード	xxxx xxxx H	0000 0100 H
リード	xxxx xxxx H	0000 0080 H
リード/ライト	xxxx xxxx H	0000 0080 H
コード	xxxx xxxx H	0010 0000 H

メモリ情報

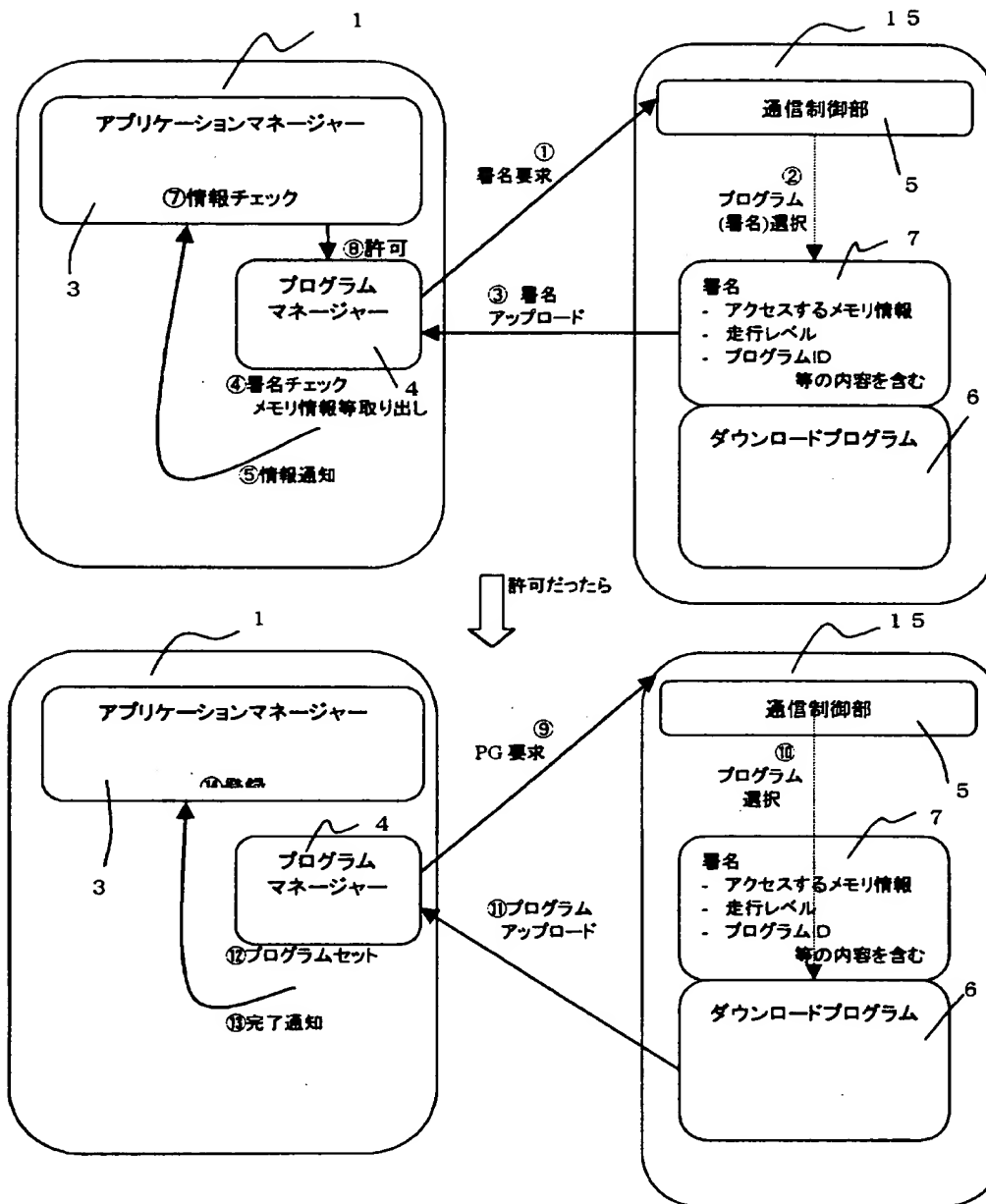
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 システム L S I において、セキュリティを維持しつつ、新規プログラムのインストールを可能とする。

【解決手段】 プログラム（６）の署名データ（７）を受信するステップと、署名データ（７）からインストールされている他のプログラムとの干渉をチェックするステップと、干渉の無いプログラムのインストールを許可するステップとを有する。インストールするプログラムから署名データを申告させ、これにより、プログラム間の干渉チェックを行い、認証を行って、干渉のあるプログラムのインストールを阻止する。又、干渉の無いプログラムのインストールを実行する。このため、セキュリティの高いプログラムを保護しつつ、新規なプログラムのインストールが可能となる。

【選択図】 図４

認定・付加情報

特許出願の番号	特願 2000-199265
受付番号	50000824362
書類名	特許願
担当官	風戸 勝利 9083
作成日	平成 12 年 7 月 6 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社

【代理人】

申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	林 恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	土井 健二

出願人履歴情報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社